



勒索軟體辨識與解密工具

Version 1.0

2021 年 7 月 9 日

TLP: WHITE

1. 簡介

加密勒索軟體 Ransomware 為一種透過資料加密手法讓受害者失去資料存取或系統的控制的惡意程式，且如不支付贖金給犯罪組織，則將無法取回受加密的資料。因犯罪組織利用這種不法模式獲利，也是其被稱為「勒索軟體」的原因。

現今的勒索軟體精密複雜且侵入性強大，透過發展各種攻擊手段與支援多國語言、跨平台等方式感染受害者設備。目前防毒軟體廠商對於部分勒索軟體已有可應對的免費解密工具，如不慎受到勒索軟體攻擊，可先參考本篇第二章節，辨識勒索軟體名稱後，透過第三章節的解密工具清單，搜尋是否有可支援的解密工具。

2. 勒索病毒種類辨識

勒索軟體種類眾多，為了取得對應的解密工具，需先正確地辨識勒索軟體名稱。本篇提供以下線上勒索軟體辨識服務，可透過提供「勒索內容」(如:勒索訊息、勒索電子郵件、網站網址等)與「被加密的檔案」進行特徵比對，判定勒索軟體名稱。

1. ID Ransomware

由 MalwareHunterTeam 提供，可辨識超過 1000 種勒索軟體。使用者可透過上傳加密檔案、勒索訊息(如無勒索訊息，可提供勒索電子郵件、網站網址)，即可進行辨識。網頁上傳介面如圖 1 所示。勒索軟體名稱辨識結果示意圖如圖 2 紅框處所示。

網址請參考：

ID Ransomware 官網：<https://id-ransomware.malwarehunterteam.com/index.php>

圖 1、ID Ransomware 上傳頁面

Upload Files

Ransom Note ?

The file that displays the ransom and payment information.

選擇檔案 未選擇任何檔案

Upload

Sample Encrypted File ?

A file which has been encrypted, and cannot be opened.

選擇檔案 未選擇任何檔案

Addresses

Optionally, you may enter any email addresses or hyperlinks the ransomware gives you for contact (if there is no ransom note).

圖 2、ID Ransomware 勒索軟體名稱的辨識結果示意圖(紅框處)



The screenshot shows the ID Ransomware website interface. At the top, there is a red header with the text "ID Ransomware" and a menu icon. Below the header, there is a large grey box containing a padlock icon with a green question mark, the title "ID Ransomware", and the instruction "Upload a ransom note and/or sample encrypted file to identify the ransomware that has encrypted your data." Below this, there is a quote: "Knowing is half the battle!" by "GI Joe".

Below the grey box, it says "1 Result". A green bar highlights the result: "TeslaCrypt 2.x". Below this, there is a green checkmark and the text "This ransomware is decryptable!". Underneath, it says "Identified by:" followed by a bullet point: "sample_extension: .ccc". At the bottom, there is a red link: "Click here for more information about TeslaCrypt 2.x". The text "TeslaCrypt 2.x" in the link is highlighted with a red box.

2. Crypto Sheriff

由 The No More Ransom Project 提供，可辨識勒索病毒並提供對應的免費解密工具。使用者可透過上傳兩個加密檔案、上傳勒索訊息檔案或是提供勒索訊息內容的電子郵件、網站網址、洋蔥網路網址、比特幣網址，即可進行辨識。上傳網頁介面如圖 3 所示。結果示意圖如圖 4 所示。

網址請參考：

No More Ransom 官網：https://www.nomoreransom.org/crypto-sheriff.php?lang=zht_Hant

圖 3、No More Ransom 解碼警長頁面

請填寫下列表格，以協助我們找出您的裝置所感染的勒索軟體種類。這些資訊將幫助我們查詢現在是否有解鎖工具可解決您的感染問題，若有，我們會將解鎖工具的下載連結提供給您。

* 若您將檔案上傳並進行掃描，代表您接受本計畫之資料提供條款。

上傳加密檔案 (檔案大小上限為1MB)

請輸入任何在勒索訊息中所看到的電子郵件、網站網址、洋蔥網路網址與/或比特幣網址。注意：請留意拼寫是否正確。

從電腦選取第一個檔案

從電腦選取第二個檔案

或是上傳罪犯在您裝置中所留下的勒索訊息檔案 (檔案格式需為txt或是html)

馬上找出勒索軟體類型!

圖 4、解碼警長勒索軟體名稱辨識結果示意圖 (紅框處)

NO MORE RANSOM!

Crypto Sheriff Ransomware: Q&A Prevention Advices Decryption Tools Report a Crime About the Project

TESLACRYPT V.4

You have been infected by **TeslaCrypt v.4**. We can help you! Good news!

Step 1: READ FIRST and DOWNLOAD

Important! Before downloading and starting the solution, click the **READ FIRST** and read the manual. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do that if you

DOWNLOAD

Step 2: Report a crime

3. 解密工具

勒索軟體名稱確認之後，可透過本章節所提供之解鎖工具網頁清單，搜尋勒索軟體名稱或是瀏覽解密工具清單找到對應的解密工具，少數勒索軟體有機會使用以下工具嘗試解密。勒索軟體名稱辨識方式請參考本篇第二章節。

1. No More Ransom 解鎖工具

由 No More Ransom Project 提供。使用者可透過搜尋勒索軟體名稱(紅框處)或是瀏覽解鎖工具列表(藍框處)(圖 5)，查看工具使用指南與下載(圖 6)。

網址請參考：

No More Ransom 官網: https://www.nomoreransom.org/zht_Hant/decryption-tools.html

圖 5、No More Ransom 解鎖工具列表與搜尋頁面

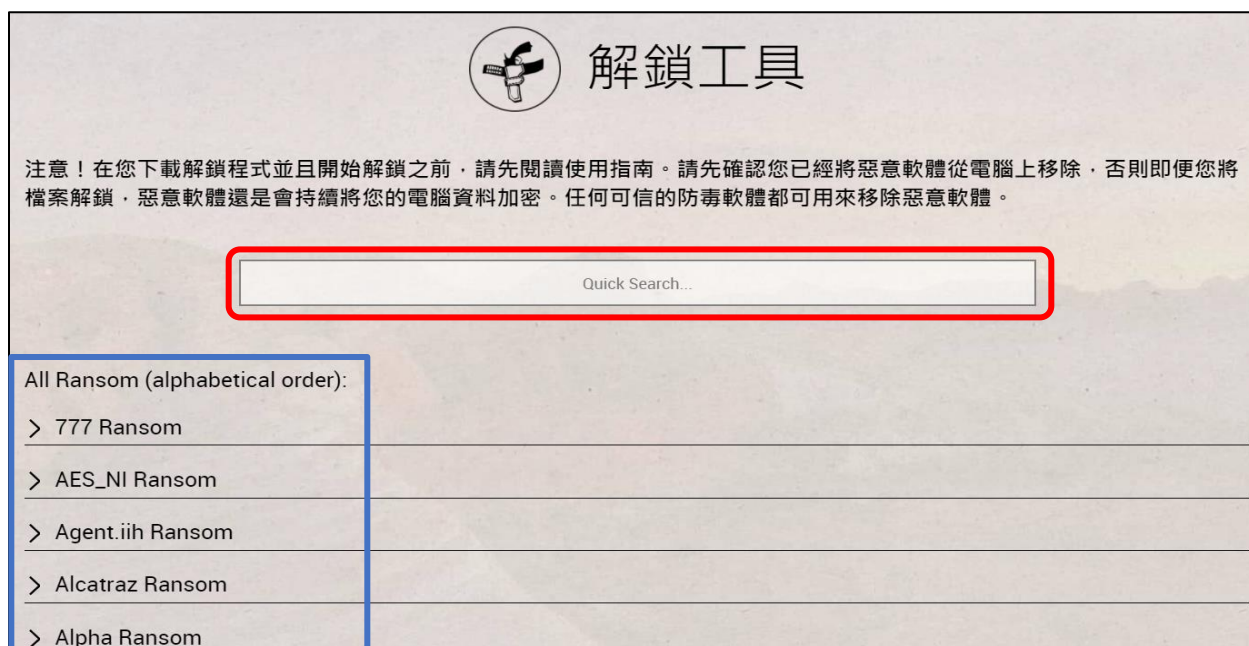


圖 6、No More Ransom 解鎖工具之說明、使用指南與工具下載連結頁面

All Ransom (alphabetical order):

- > 777 Ransom
- > AES_NI Ransom
- ✓ Agent.iih Ransom
- > Alcatraz Ransom
- > Alpha Ransom
- > Amnesia Ransom
- > Amnesia2 Ransom

Rakhni解鎖工具是設計來解鎖由Agent.iih勒索軟體所加密的檔案。

更多資訊請詳閱以下內容 [使用指南](#)

[下載](#)

工具由 Kaspersky Lab 製作

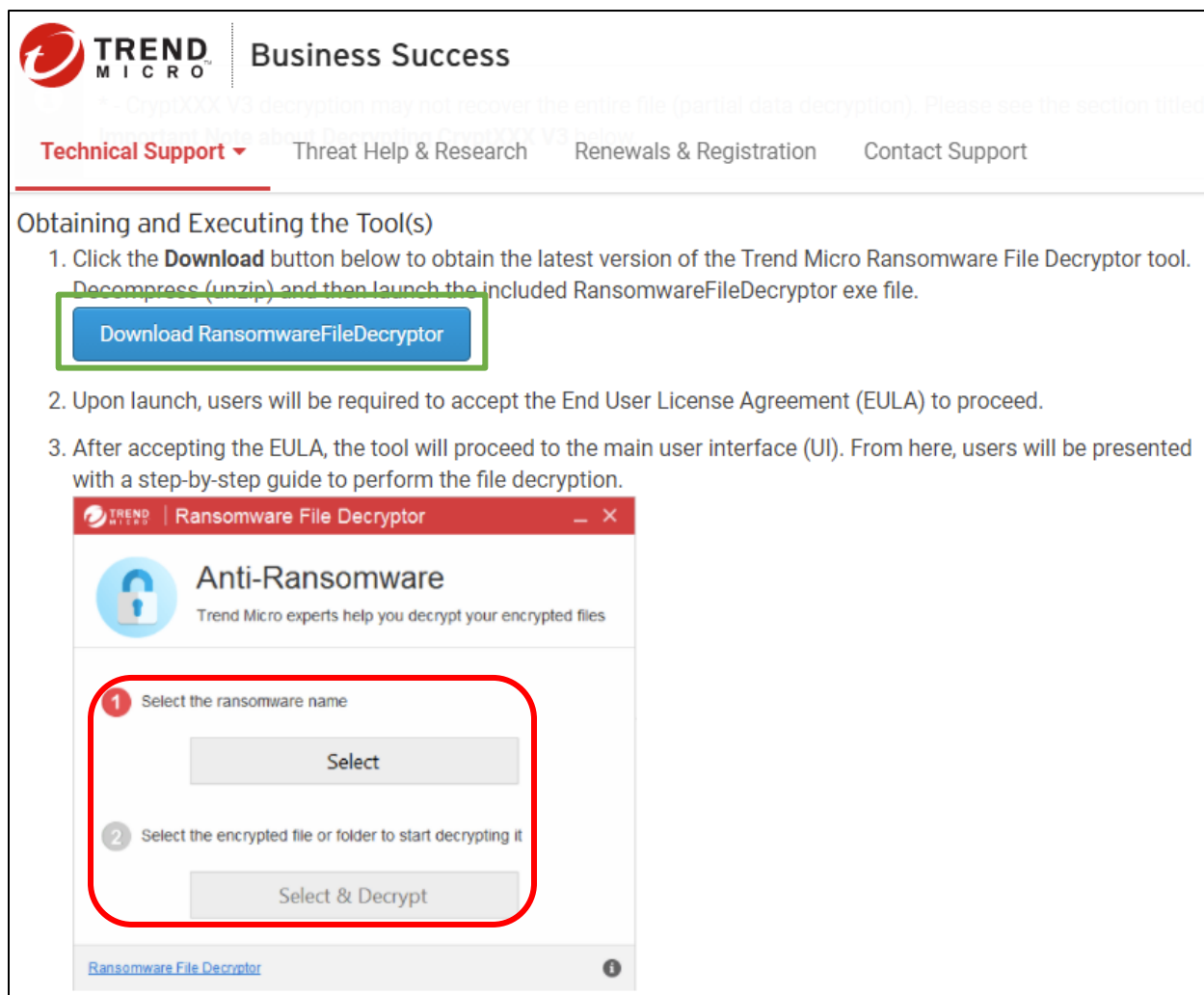
2. Trend Micro Ransomware File Decryptor

由 Trend Micro 提供。使用者可下載 (綠框處) 與執行 RansomwareFileDecryptor 工具，選擇勒索軟體名稱與欲解密的檔案或資料夾進行解密 (紅框處)。頁面如圖 7 所示。

網址請參考：

Trend Micro 官網：<https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor>

圖 7、Trend Micro Ransomware File Decryptor 下載與說明頁面



The screenshot displays the Trend Micro Business Success portal. At the top, there is a navigation bar with 'Technical Support' selected. The main content area is titled 'Obtaining and Executing the Tool(s)' and contains two numbered steps. Step 1 instructs the user to click the 'Download' button, which is highlighted with a green box in the image. Step 2 instructs the user to accept the EULA. Step 3 instructs the user to follow a step-by-step guide. Below the text, there is a screenshot of the 'Ransomware File Decryptor' application window. The window title is 'Ransomware File Decryptor' and the main heading is 'Anti-Ransomware'. The interface shows two steps: '1 Select the ransomware name' with a 'Select' button, and '2 Select the encrypted file or folder to start decrypting it' with a 'Select & Decrypt' button. A red box highlights these two steps in the application window.

3. 卡斯基 Free Ransomware Decryptors

由卡斯基提供。使用者可瀏覽解密工具列(藍框處)表或是搜尋名稱(紅框處)，下載所需之解密工具進行解密。搜尋畫面與列表如圖 8 所示。

網址請參考：

卡斯基官網：<https://noransom.kaspersky.com/>

圖 8、卡斯基 Free Ransomware Decryptor 解密工具搜尋與瀏覽頁面



The screenshot shows the Kaspersky website for free ransomware decryptors. The page is in Chinese and includes a search bar, a list of tools, and a '常見問答' (FAQ) button. The search bar is highlighted with a red box, and the list of tools is highlighted with a blue box.

免費勒索软件解密器

欢迎访问No Ransom，在这里您可以找到最新的解密器、勒索软件删除工具以及防御勒索软件的相关信息。

什么是勒索软件？勒索软件是一种恶意软件（木马或其他类型的病毒），它能锁定用户设备或加密用户文件，然后通知用户必须支付赎金才能拿回自己的数据。赎金并不低，但不能保证一定能成功解密。如果您是勒索软件的受害者，请试试我们的免费解密工具，它能帮助您数字生活恢复正常。

首先删除勒索软件（您可以使用“卡斯基安全软件”），否则它会再次锁定您的系统。

在启动解密器之前，请先阅读相关操作指南。

键入文件扩展名、电子邮件或锁定的屏幕上提示的其他所有信息

搜索

工具名称	描述	更新时间
Shade Decryptor	解密受所有Shade版本影响的文件 操作指南	30 Apr 2020
Rakhni Decryptor	解密被Rakhni、Agent.iih、Aura、Autoit、Pletor、Rotor、Lamer、Cryptokluchen、Lortok、Democry、Bitman、TeslaCrypt (V3和V4)、Chimera、Crysis (V2和V3) 锁定的文件。最新更新：解密Cryakl、Fonix 勒索软件 操作指南	3 Feb 2021

4. AVG 免費軟體解密工具

由 AVG 提供。使用者可瀏覽解密工具列表(圖 9)(藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 10)。

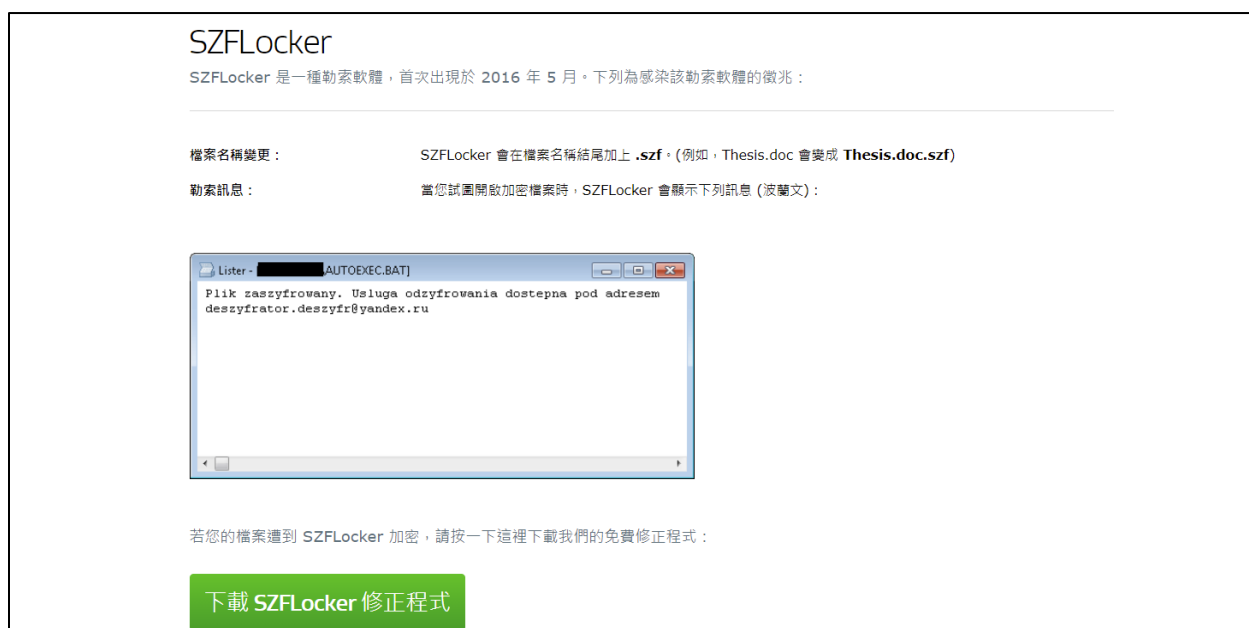
網址請參考：

AVG 官網：<https://www.avg.com/zh-tw/ransomware-decryption-tools>

圖 9、AVG 免費勒索軟體解密工具列表頁面



圖 10、工具說明、勒索訊息畫面與修正程式下載連結(示意圖)



5. EMSI SOFT Free Ransomware Decryption Tools

由 EMSI SOFT 提供。使用者可瀏覽解密工具列表(藍框處)，下載所需解密工具(圖 11)。

網址請參考：

EMISI SOFT 官網：<https://www.emsisoft.com/ransomware-decryption-tools/free-download>

圖 11、EMSI SOFT Free Ransomware Decryption Tool 解密工具列表頁面



Free Ransomware Decryption Tools

Unlock your files without paying the ransom

[Jun, 11, 2021] - Version: 2.1.0.0

Emsisoft Decryptor for Avaddon

24342 downloads

The Avaddon ransomware encrypts victim's files using AES-256 and RSA-2048, and appends a random extension.

Please note the decryptor may take up to a minute on the first encrypted file in order to determine the correct key for your files. All other files encrypted by the same key will decrypt much faster.

6. McAfee Ransomware Recover (Mr²)

Mr² 為 McAfee 開發之解密工具，採取指令列介面，且定期更新支援的勒索軟體主類。使用者可透過圖 12 下載安裝 Mr² (綠框處)，執行後可透過指令檢視支援解密的勒索軟體列表與進行解密，如圖 13 所示。

網址請參考：

McAfee 官網：<https://www.mcafee.com/enterprise/zh-tw/downloads/free-tools/ransomware-decryption.html>

使用 Mr2 破解勒索軟體 Stampado 之範例與說明：

Stampado 勒索訊息如圖 14 所示，內容提示受害者需透過攻擊者電子郵件 (圖 14 紅框處) 聯繫以取得解鎖碼輸入 (圖 14 綠框處) 進行檔案解密。

- 1) 啟動 Mr2 後，輸入 'MfeDecrypt -list' 指令 (圖 15 綠框處) 搜尋 'Stampado' 勒索軟體的解密工具 (圖 15 紅框處)
- 2) 執行 'MfeDecrypt -get stampado -ver 1.0.0' 指令下載 Stampado 解密工具。(圖 16 紅框處)
- 3) 執行 'MfeDecrypt -about stampado -ver 1.0.0' 指令查看解密工具使用方式 (圖 17 紅框處)。
- 4) 透過 'MfeDecrypt -run stampado -ver 1.0.0 -args "-e FileUnlocker64@mail2tor.com' 命令執行解密工具 (圖 18 紅框處)，提供圖 14 紅框處的勒索聯絡電子郵件，取得解鎖碼 (圖 18 綠框處)，並於圖 13 的勒索訊息畫面輸入解鎖碼進行檔案解密。

圖 12、McAfee Ransomware Recover (Mr2) 下載頁面



McAfee Ransomware Recover (Mr²)

McAfee Ransomware Recover (Mr²) will be regularly updated as the keys and decryption logic required to decrypt files held for ransom become available. This tool can unlock user files, applications, databases, applets, and other objects encrypted by ransomware.

We intend for this framework to be freely available to all. This allows anyone in the security community who may have decryption keys and decryption logic to avoid the burden of developing a decryption framework.

[Download McAfee Ransomware Recover \(Mr²\) for 32-bit systems >](#)

[Download McAfee Ransomware Recover \(Mr²\) for 64-bit systems >](#)

[How to use McAfee Ransomware Recover \(Mr²\)](#)

圖 13、Mr2 執行畫面，包含工具指令與說明

```

McAfee Ransomware Decryption Tool

Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC

Usage: MfeDecrypt <command> [arguments...]
Supported commands and their arguments are:

MfeDecrypt -help
Show MfeDecrypt help text.

MfeDecrypt -list
Show list of all decryption tools available.

MfeDecrypt -get <name> [-ver version]
Download latest version of decryption tool (or specific version).

MfeDecrypt -run <name> [-ver version] [-args "arguments in double quotes"]
Run latest downloaded decryption tool (or specific version) with given arguments (when needed)
Tool must be downloaded using "-get" command before running.

MfeDecrypt -about <name> [-ver version]
Show help text of latest downloaded decryption tool (or specific version).
Tool must be downloaded using "-get" command before running.

For example:
To download a ransomware decryption tool and run it:
1. Get list of all available tools: MfeDecrypt -list
2. Pick tool name and version from list. For example, stampado 1.0.0
3. Download stampado: MfeDecrypt -get stampado -ver 1.0.0
4. Get stampado help: MfeDecrypt -about stampado -ver 1.0.0
5. Run stampado: MfeDecrypt -run stampado -ver 1.0.0 -args "-e FileUnlocker64@mail2tor.com"

```

圖 14、Stampado 勒索訊息 (示意圖)

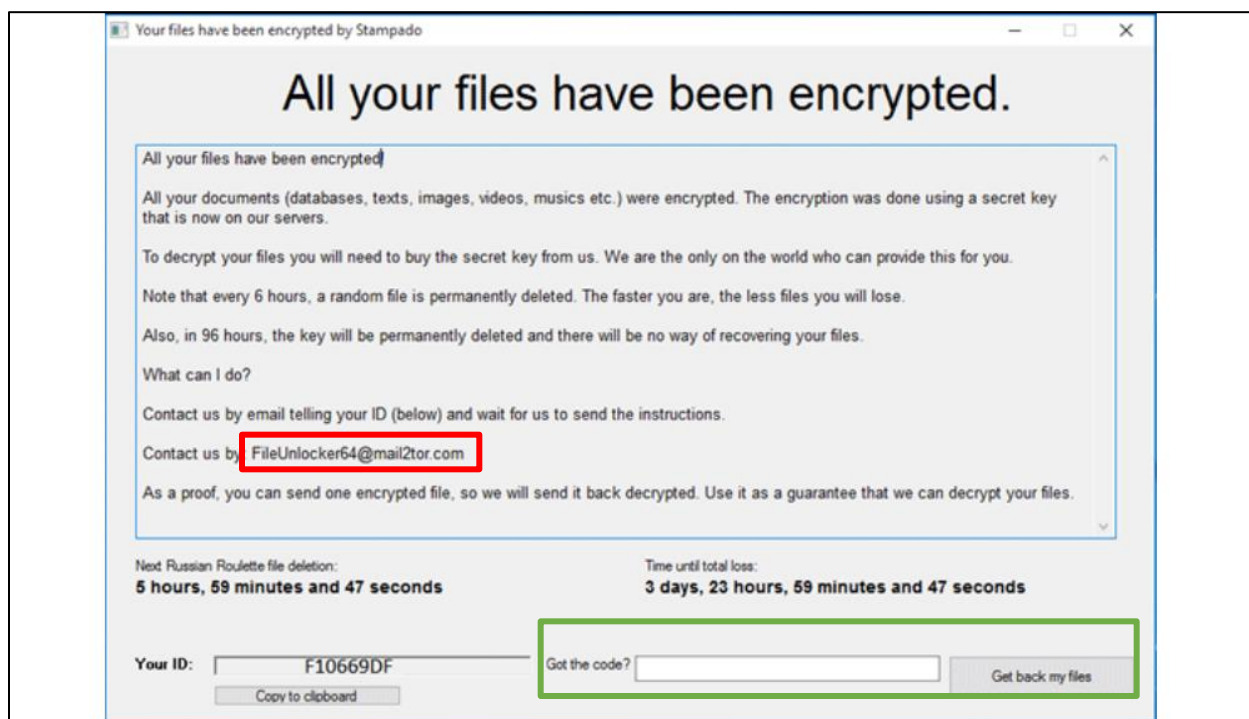
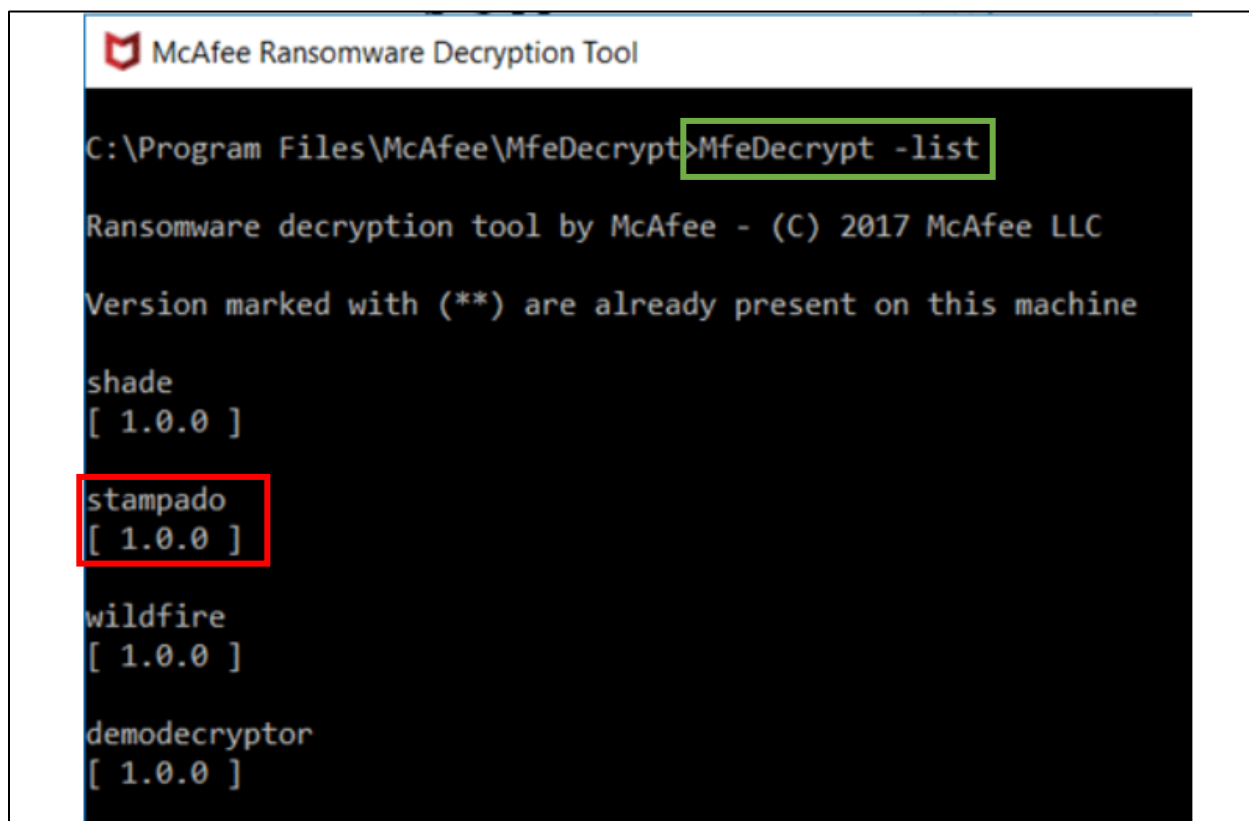


圖 15、Mr2 支援 Stampado 解密與顯示所有勒索軟體解密支援的命令 (示意圖)



```
McAfee Ransomware Decryption Tool

C:\Program Files\McAfee\MfeDecrypt>MfeDecrypt -list

Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC

Version marked with (**) are already present on this machine

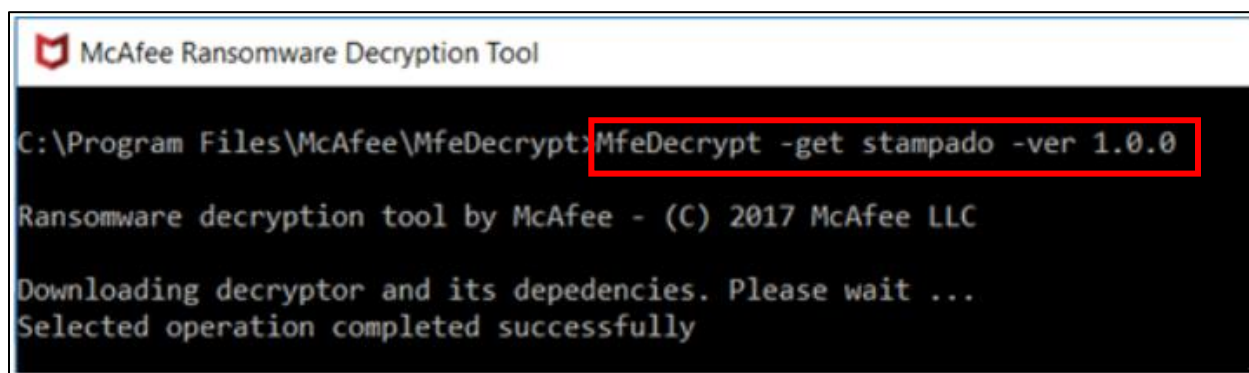
shade
[ 1.0.0 ]

stampado
[ 1.0.0 ]

wildfire
[ 1.0.0 ]

demodecryptor
[ 1.0.0 ]
```

圖 16、下載勒索軟體 Stampado 解密工具的命令 (示意圖)



```
McAfee Ransomware Decryption Tool

C:\Program Files\McAfee\MfeDecrypt>MfeDecrypt -get stampado -ver 1.0.0

Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC

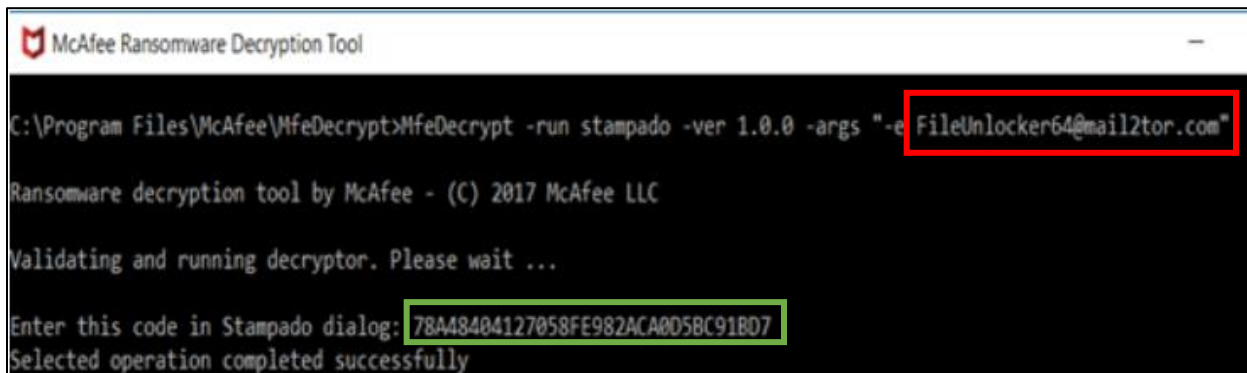
Downloading decryptor and its dependencies. Please wait ...
Selected operation completed successfully
```

圖 17、Stampado 解密工具命令使用方式 (示意圖)



```
McAfee Ransomware Decryption Tool  
C:\Program Files\McAfee\MfeDecrypt>MfeDecrypt -about stampado -ver 1.0.0  
Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC  
Validating and running decryptor. Please wait ...  
Usage:  
MfeDecrypt.exe -run stampado -ver 1.0.0 -args "-e <email_id_displayed>"  
Selected operation completed successfully
```

圖 18、取得 Stampado 解鎖碼 (示意圖)



```
McAfee Ransomware Decryption Tool  
C:\Program Files\McAfee\MfeDecrypt>MfeDecrypt -run stampado -ver 1.0.0 -args "-e FileUnlocker64@mail2tor.com"  
Ransomware decryption tool by McAfee - (C) 2017 McAfee LLC  
Validating and running decryptor. Please wait ...  
Enter this code in Stampado dialog: 78A48404127058FE982ACA005BC91B07  
Selected operation completed successfully
```

7. Avast Free Ransomware Decryption Tools

由 Avast 提供。使用者可瀏覽解密工具列表(圖 19)(藍框處)，檢視解密工具說明與下載修正程式進行解密(圖 20)。

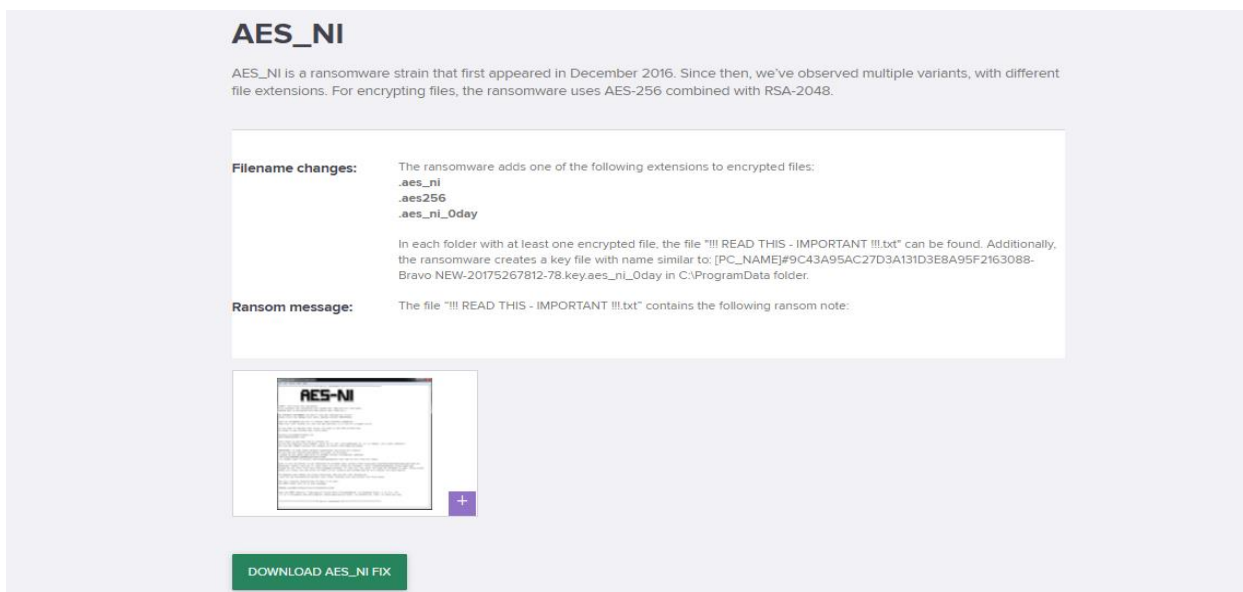
網址請參考：

Avast 官網：<https://www.avast.com/ransomware-decryption-tools>

圖 19、Avast Free Ransomware Decryption Tool 解碼工具列表頁面



圖 20、解密工具說明、勒索訊息截圖與下載連結(示意圖)



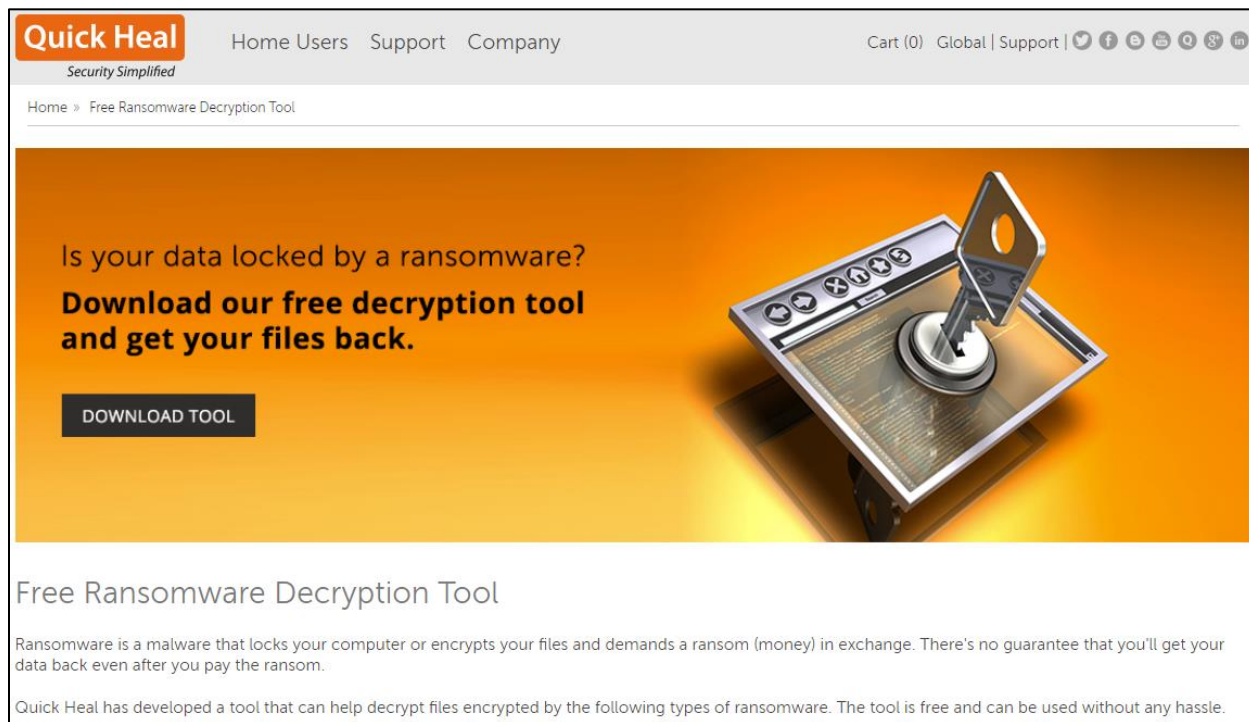
8. Quick Heal Free Decryption Tool


由 Quick Heal 提供。使用者可下載支援多種勒索軟體解密的工具進行解密(圖 21)。執行工具後，會自動進行掃描加密檔案進行解密。

網址請參考：

Quick Heal 官網: <https://www.quickheal.com/free-ransomware-decryption-tool/>

圖 21、Quick Heal Free Ransomware Decryption Tool 解密工具下載頁面



Quick Heal Home Users Support Company Cart (0) Global | Support | 

Security Simplified

Home » Free Ransomware Decryption Tool

Is your data locked by a ransomware?
**Download our free decryption tool
and get your files back.**

DOWNLOAD TOOL

Free Ransomware Decryption Tool

Ransomware is a malware that locks your computer or encrypts your files and demands a ransom (money) in exchange. There's no guarantee that you'll get your data back even after you pay the ransom.

Quick Heal has developed a tool that can help decrypt files encrypted by the following types of ransomware. The tool is free and can be used without any hassle.

9. MDS Ransomware Decryption Tools

由 MDR 提供。使用者可瀏覽解密工具列表，下載所需解密工具進行解密，如圖 22 所示。

網址請參考：

MDS 官網: <https://www.mdsny.com/decryption-tools/>

圖 22、MDS Ransomware Decryption Tools 解密工具列表

777 Ransom	+	Decrypt 777 🔑
AES_NI Ransom	+	Decrypt AES_NI 🔑
Agent.iih Ransom	+	Decrypt Agent.iih 🔑
Alcatraz Ransom	+	Decrypt Alcatraz 🔑
Amnesia Ransom	+	Decrypt Amnesia 🔑
Amnesia2 Ransom	+	Decrypt Amnesia2 🔑